DEFINITION OF DEFENSE-IN-DEPTH

ISSUE: How to specify "defense-in-depth" for non-light-water reactors (non-LWRs), (Should a description be developed?)

BACKGROUND:

In SECY-03-0047, "Policy Issues Related to Licensing Non-Light-Water Reactor Designs," dated March 28, 2003 (ML030160002), with respect to defense-in-depth, the staff recommended that the Commission take the following actions:

- Approve the development of a policy statement or description (e.g., white paper) on defense-in-depth for nuclear power plants to describe:
  - the objectives of defense-in-depth (philosophy)
  - the scope of defense-in-depth (design, operation, etc.)
  - the elements of defense-in-depth (high level principles and guidelines)

  The policy statement or description would be technology neutral and risk-informed and would be useful in providing consistency in other regulatory programs (e.g., Regulatory Analysis Guidelines).

- Develop the policy statement/description through a process involving stakeholder review, input, and participation.

In the June 26, 2003, staff requirements memorandum (SRM), the Commission approved development of a description of defense-in-depth for incorporation into the policy statement on the use of probabilistic risk assessment (PRA).

DISCUSSION:

The concept of defense-in-depth is fundamental to the NRC's safety philosophy that there must be adequate measures to deal with uncertainty. Regulatory Guide 1.174 ("An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," Revision 1, November 2002, ML020810773) states: "The defense in depth philosophy .....has been and continues to be an effective way to account for uncertainties in equipment and human performance." In the Commission's Strategic Plan for FY 2004-20 defense-in depth is described as "an element of the NRC's Safety Philosophy that employs successive compensatory measures to prevent accidents or lessen the effects of damage if a malfunction or accident occurs at a nuclear facility. The NRC's Safety Philosophy ensures that the public is adequately protected and that emergency plans surrounding a nuclear facility are well conceived and will work. Moreover, the philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility." On a number of occasions, the Advisory Committee on Reactor Safeguards (ACRS) examined defense-in-depth as a means of dealing with uncertainty.

A summary of the objectives of defense-in-depth can be stated as the ability to:

- compensate for potential adverse human actions (this includes commission as well as omission) and component failures,
- maintain the effectiveness of barriers by averting damage to the plant and the barriers themselves, and
- protect the public and environment from harm in the event that these barriers are not fully effective.

The staff's current approach in the technology-neutral framework for specifying defense-in-depth has three key elements: (1) development of defense-in-depth principles, (2) development of a defense-in-depth model for application, and (3) guidance on the implementation of the defense-in-depth model.

Defense-in-Depth Principles

To achieve the defense-in-depth objectives, and therefore assure public safety despite uncertainties, the staff is proposing some fundamental principles. The first principle requires that *measures against intentional as well as inadvertent events are provided***.** This is intended to ensure that in the application of defense-in-depth human initiated (e.g., security), as well as random events and natural phenomena, are considered.

From the first principle of defense-in-depth, the staff is developing four more defense-in-depth principles.

The design should provide accident prevention and mitigation capability. Accident prevention and mitigation capability should be provided such that there is no undue emphasis on either' at the expense of the other, for maintaining the plant in a safe condition given various challenges. Specific measures are sometimes seen as either preventive or mitigative depending on the point in the event sequence and the point of view of the observer. Often prevention is emphasized relative to mitigation because preventive measures are usually more economical, prevention avoids having to deal with the phenomenological uncertainties that arise once an accident progresses, etc. From a defense-in-depth standpoint such an emphasis is acceptable as long as it does not result in an exclusive reliance on prevention with a neglect of mitigative features.

Accomplishment of key safety functions should not be dependent upon a single element of design, construction, maintenance or operation. Redundancy, diversity, and independence in structures, systems, and components (SSCs) and actions will ensure that no key safety functions will be dependent on a single element (i.e., SSC or action) of design, construction, maintenance or operation. The key safety functions include: control of reactivity, removal of decay heat, and the functionality of physical barriers to contain the release of radioactive materials. In addition, hazards such as fire, flooding, and seismic events which have the potential to defeat redundancy, diversity, and independence, need to be considered.

Uncertainties in SSCs and human performance should be accounted for such that reliability and risk goals can be met. Allocation of risk goals for a new design must include uncertainty. The setting of success criteria for the achievement of safety functions should be set, and the

calculations that show they have been met should be performed, in such a way that uncertainties are accounted for with a high level of confidence. For future reactors this needs to be accomplished without the benefit of reviewing past performance. The role of safety margins is important here in achieving a robust design. Both physical and temporal margins should be incorporated in the plant equipment and procedures.

Plants should be sited in areas that meet the intent of Part 100 and are consistent with the principles for siting established in Regulatory Guide 4.7 ("General Site Suitability Criteria for Nuclear Power Plants). The location of regulated facilities should be chosen so as to serve the protection of public health and safety. Consideration of population densities and the proximity of natural and man-made hazards in the siting of plants can provide further assurance that hazards to the public are minimized. For reactors, this principle is also intended to ensure that accident management, including emergency preparedness, remains a fundamental element of defense-in-depth. However, the staff recognizes that the scope and nature of offsite emergency preparedness activities could be different for future reactors, due to factors such as reactor size (i.e., power level), location, level of safety (i.e., likelihood of release), magnitude and chemical form of the radionuclide release, and timing of releases (i.e., long-term response).

Defense-in-Depth Model

The model of defense-in-depth which the staff is recommending for application to new reactors incorporates both deterministic and probabilistic elements. The deterministic part of the model mainly addresses completeness uncertainties by asking the question, "What if this barrier or safety feature fails?" without relying on a quantitative estimate of the likelihood of such a failure. As a result, the deterministic element is defined by protective strategies that are successive measures designed to protect public health and safety even if some of the strategies fail. The protective strategies of the technology-neutral framework are to ensure Physical Protection, maintain Barrier Integrity, limit Initiating Event Frequencies, assure adequate reliability of Protective Systems, and provide Accident Management. In addition, the deterministic element imposes specific qualitative requirements to be included in the regulations to ensure that the accomplishment of key safety functions are not dependent upon a single element of plant design construction, maintenance or operation.

The probabilistic part of the model seeks to evaluate the uncertainties in the analysis and to determine what steps should be taken to compensate for those uncertainties. The probabilistic elements address primarily modeling and parameter uncertainties, and establish specific quantitative performance goals, such as equipment reliability goals, that compensate for the calculated uncertainty.

The staff's defense-in-depth model uses a deterministic approach at a high level by requiring that all the protective strategies are included. Within each protective strategy a probabilistic approach is used to determine how much defense-in-depth is needed to achieve the desired quantitative goals on initiating event frequency and safety system reliability, including uncertainty.

Implementation of the Defense-in-Depth

The staff's approach for implementation of the above model relies on the application of the defense-in-depth principles as qualitative criteria to be adhered to, and the use of a PRA for achieving quantitative risk goals. Inclusion of all the protective strategies assures some

protection against completeness uncertainty. Within each strategy, a probabilistic defense-in-depth element is applied to ensure adequate performance in meeting the objective of the strategy. The systems, barriers and actions used in the performance of the safety functions associated with the protective strategy are examined in terms of deterministic and probabilistic elements of defense-in-depth. Quantitative risk information is be used, where possible, to assess the degree of conformance and the need for additional defense-in-depth measures (e.g., redundancy, diversity, safety margins).

Monitoring and feedback are essential aspects of this process, since the validity of initial design assumptions, and of design changes made as part of the outlined steps, will be established by the actual operation of the reactor. Additional hardware or procedural changes may result from this feedback. This is especially important for the new and innovative designs for which there is no operating experience.

The staff envisions whole process of applying defense-in-depth as an iterative process, a series of steps, that is expected to be used initially by the designer and ultimately by the designer and regulator to develop the emerging design. As the design evolves the PRA will also be able to be developed to greater detail.

PROBABILISTIC APPROACH FOR ESTABLISHING THE LICENSING BASIS

ISSUE: To what extent can a probabilistic approach be used to establish the licensing basis?

BACKGROUND:

In SECY-03-0047, the staff recommended that the Commission take the following actions with respect to using a probabilistic approach to establish the licensing basis

- Modify the Commission's guidance, as described in the SRM of July 30, 1993, to put greater emphasis on the use of risk information by allowing the use of a probabilistic approach in identifying events to be considered in the design, provided there is sufficient understanding of plant and fuel performance and deterministic engineering judgement is used to bound uncertainties.

- Allow a probabilistic approach for the safety classification of structures, systems, and components.

- Replace the single failure criterion with a probabilistic (reliability) criterion.

These recommendations are consistent with a risk-informed approach. The recommendation expands the use of PRA into forming part of the basis for licensing and thus put greater emphasis on PRA quality, completeness, and documentation.

In the June 26, 2003, SRM, the Commission approved the staff recommendation.

DISCUSSION:

As part of developing the technology-neutral framework for new plant licensing, draft guidance has been developed related to implementation of a probabilistic approach for establishing the licensing basis. This draft guidance is intended for staff use in developing technology-neutral requirements based upon the framework guidance. Summarized below are the key elements of the draft guidance developed for implementation of a probabilistic approach for establishing the licensing basis, which the staff proposes for use in developing the technology-neutral requirements:

Probabilistic Event Selection Criteria

The following criteria are proposed for the categorization of event scenarios (identified in a design specific PRA) which must be considered in the design

- frequent $\geq 10^{-2}$/plant year (mean value)
- infrequent $<10^{-2}$/plant year but $\geq 10^{-5}$/plant year (mean value)
- rare $<10^{-5}$/plant year but $\geq 10^{-7}$/plant year (mean value)

These proposed criteria are intended to ensure that a sufficiently broad spectrum of event scenarios are considered consistent with the safety expectations expressed in the

Commission's Safety Goal Policy Statement. It is proposed to use each of these event categories as follows:

- Frequent event scenarios represent the anticipated operational occurrence (AOOs) range from which AOOs will be selected and will have to meet a deterministic dose criteria of 100 mrem as described in Part 20.

- Infrequent event scenarios represent the design basis accident (DBAs) range from which DBAs will be selected and will have to meet deterministic dose criteria associated with siting (e.g., 25 rem total effectiveness dose equivalent of the EAB).

- Rare event scenarios will be used for assessing emergency preparedness, as well as be used (along with the frequent and infrequent events) in assessing overall plant risk.

- Event scenarios of lower frequency than the rare category will not have to be considered for licensing purposes; however, it will also be necessary for an applicant to show that catastrophic initiating events (e.g., reactor pressure vessel rupture) that can cause the breach of all barriers to radiation release must be kept below a frequency of 10^{-7}/plant year.

Probabilistic Safety Classification

The staff proposes the safety classification of SSCs be based upon their risk importance. PRA results would be analyzed using conventional risk importance measures (e.g., risk achievement worth-where the failure rate of the SSC is set to one to determine the change in risk) and criteria established to categorize the importance of the SSC. The risk importance measures and criteria are yet to be developed, but will build upon the work done in support of the 10 CFR 50.69 rulemaking.

Single-Failure Criterion:

The single failure criterion will be replaced with the event sequences from the design specific PRA. Whichever number of failures are contained in those event sequences, the design and safety analysis will also need to consider.

As a final consideration, it is expected that designs that are licensed using a probabilistic approach will need to feedback operating experience into their PRA and maintain it as a living document. As such, event sequences and SSC importance may change over time potentially affecting the event categorization, AOO and DBA selection and analysis and safety classification of SSCs. Accordingly, a process to incorporate such changes into the license (for both certified and non-certified designs) will need to be developed.

USE OF SCENARIO-SPECIFIC SOURCE TERMS FOR LICENSING DECISIONS

ISSUE: Under what conditions should scenario-specific accident source terms be used for licensing decisions?

BACKGROUND:

In SECY-03-0047, with regard to using scenario-specific accident source term for licensing decisions, the staff recommended that the Commission take the following action:

- Retain the Commission's guidance contained in the July 30, 1993, SRM that allows the use of scenario-specific source terms, provided there is sufficient understanding and assurance of plant and fuel performance and deterministic engineering judgement is used to bound uncertainties.

This recommendation will allow credit to be given for the unique aspects of plant design and builds upon the recommendation under the issue on the use of PRA. Furthermore, this approach is consistent with prior Commission and ACRS views. However, this approach is also dependent upon understanding fuel and fission product behavior under a wide range of scenarios and on ensuring fuel and plant performance is maintained over the life of the plant.

In the June 26, 2003, SRM, the Commission approved the staff's recommendation.

DISCUSSION:

As part of developing the technology neutral framework for future plant licensing, draft guidance has been developed and included in the framework related to implementation of a scenario specific source term approach. This draft guidance is intended for staff use when developing technology-neutral requirements based upon the framework. Summarized below are the key elements of the draft guidance developed for implementation of scenario specific licensing source terms, which the staff intends to incorporate in the technology-neutral requirements:

- The scenarios to be used for the source term evaluation are to be selected from a design specific probabilistic risk assessment, with due consideration of uncertainties, as discussed under the issue addressing the use of a probabilistic approach for establishing the licensing basis.

- The source term calculation, using the selected scenarios, should be based upon analytical tools that have been verified with sufficient experimental data to cover the range of conditions expected and to determine uncertainties.

- The source terms used for assessing compliance with dose related siting requirements should be 95% confidence level values based upon best estimate calculations with quantified uncertainties. Where uncertainties cannot be quantified, engineering judgement shall be used.

- The source terms used in assessing emergency preparedness should be mean values based upon best estimate calculations with quantified uncertainties.

- The source terms used for licensing decisions should reflect the scenario specific timing, form and magnitude of radioactive material released from the fuel and coolant. Credit may be taken for natural and/or engineered attenuation mechanisms in estimating the release to the environment, provided there is adequate technical basis to support their use.

The guidance is intended to provide a flexible, performance-based, approach for establishing scenario specific licensing source terms. However, it also puts the burden on the applicant to develop the technical bases (including experimental data) to support their proposed source terms. Applicants could, however, propose to use a conservative source term for licensing purposes (in order to reduce research and development costs and schedule), provided the use of such a source term does not result in design features or operational limits that could detract from safety.

Finally, it should be noted that in parallel with developing technology-neutral regulations, the staff also plans to develop technology-specific Regulatory Guides that will provide guidance on one acceptable way to implement the technology-neutral regulations on a specific reactor technology (e.g., high temperature gas-cooled reactors). These Regulatory Guides could provide further guidance on the use of scenario specific source terms, such as credit for attenuation mechanisms. In this regard, it is expected that some future LWR designs will also propose to use scenario specific source terms. These requests could be reviewed on a case-by-case basis using the guidance.

POSSIBLE MODIFICATIONS OF EMERGENCY PREPAREDNESS REQUIREMENTS

ISSUE: Under what conditions can the emergency preparedness requirements be modified to give credit for reactor designs with enhanced safety characteristics?

BACKGROUND:

In SECY-03-0047, the staff recommended that no change to emergency preparedness requirements be made at this time. This recommendation is consistent with the guidance contained in the Commission's July 30, 1993, SRM, and is based upon the following two considerations:

- Provision already exists in 10 CFR 50.47 (“Emergency Plans”) for accommodating the unique aspects of high-temperature gas reactors.

- In the near term, new plants are likely to be built on an existing site which conforms to current requirements.

In the longer term, the staff also recommended that the role of emergency preparedness in defense-in-depth would be addressed as part of the staff’s work to develop a policy or description of defense-in-depth which is part of the framework development, as recommended under the defense-in-depth issue. If, and when, a need for change in emergency preparedness requirements is identified, that policy or description would serve as guidance in assessing the proposed change. In the June 26, 2003, SRM, the Commission approved the staff recommendation in SECY-03-0047.

Current requirements associated with emergency preparedness (i.e., 10 CFR 50.47, and 10 CFR Part 50, Appendix E [“Emergency Planning and Preparedness for Production and Utilization Facilities”]) have been developed primarily in consideration of the risks from currently operating LWRs. However, 10 CFR 50.47 does recognize that for gas-cooled nuclear reactors and for reactors with authorized power level less than 250 Mwt, the size of the emergency planning zones (EPZs) may be determined on a case-by-case basis. This situation was the case for the Fort Saint Vrain reactor which had a 5-mile EPZ, instead of the 10-mile EPZ, that is applied to currently operating LWRs.

In the past, there have been proposals to modify current emergency preparedness requirements to give credit for designs with enhanced safety characteristics. Staff reviews and response to these proposals were provided. In general, these responses indicated that for new reactor designs, it is too early to identify specific conditions that would allow a reduction in the 10-mile plume exposure pathway EPZ. Until sufficient experience is gained on any prototype reactor, a case-by-case basis should be used to evaluate whether a requested reduction in the size of the EPZ can be allowed. This criterion would also apply to the 50-mile ingestion control pathway EPZ. Some conditions that would have particular importance would include, but would not be limited to, the following:

- consideration of the full range of accidents
- use of the defense-in-depth philosophy
- prototype operating experience is gained

- acceptance by federal, state, and local agencies
- acceptance by the public

Finally, all sixteen Planning Standards and Evaluation Criteria (A through P) in NUREG-0654/FEMA-REP-1, Rev. 1, should be addressed for any size EPZ. The specific requirements under each applicable standard could be scaled down, as appropriate, in order to account for any reduction in EPZ size. Modification of the rules or guidance documents should not occur until sufficient experience is gained in dealing with reduced EPZs.

DISCUSSION:

The staff plans to obtain stakeholder feedback on the above emergency preparedness considerations, as they relate to modifying emergency preparedness requirements to give credit for reactor designs with enhanced safety characteristics. Based upon feedback and further technical considerations, provide a recommendation to the Commission in late 2005.